FCC Computer System
Application Access Assignment Form

Employees and contractors who are requesting application access must have this form completed and returned to the Application Owner. Access must be granted in accordance with FCC Instruction 1479.2 Computer Security Program Directive.

USER INFORMATION **(To be completed by Application Owner)**	
User Name (*Print Last, First MI*):	User Name ID:
Bureau/Office or Contract Name:	Date Access Required:
Major Application Access:	Access Level:

APPLICATION RULES OF BEHAVIOR ACKNOWLEDGEMENT
(To be completed by user and returned to Application Owner when Completed)

I have received a copy of the attached Application Rules of Behavior that provide information on Federal regulations, user responsibilities and the consequences of my actions, and computer security policies and procedures. I have read and will fully comply with the rules in their entirety. I recognize that it is my responsibility to ensure that I comply with the Federal computer security policies and procedures described in the FCC Computer Security Program Directive.

Printed Name: _____ Organization: _____

Signature: _____ Date: _____

ACCESS APPROVAL

I am aware that the following access has been granted to this userID:

☐ Privileged, Administrative Account. ☐ Non-Privileged, Non-Administrative User Account

Supervisor or COTR *(Printed Name)*:	Signature: Date:
Application Security Custodian *(Printed Name):*	Signature: Date:

Return this form to the Computer Security Officer, Room 1-A325
445 12th Street, S.W., Washington, DC 20554

APPLICATION RULES OF BEHAVIOR

Passwords:

- ☐ Passwords must be at least characters long.
- ☐ Do not write down passwords.
- ☐ Do not share your passwords or accounts with others.
- ☐ Enable a password protective inactivity screensaver at your station.
- ☐ Passwords are to be changed every days.
- ☐ Use paraphrases instead of dictionary words when creating passwords.

Electronic Data/Media and Paper:

- ☐ Do not post system sensitive material in areas subject to public traffic or viewing (offices next to windows on ground floors please take special note).
- ☐ Do not transport system sensitive material in an unprotected manner.
- ☐ Lock down all sensitive unclassified material when leaving your work area.
- ☐ Protect sensitive unclassified information from alteration, disclosure or loss.
- ☐ Ensure all storage media are reformatted before they are removed for storage in a protected environment.
- ☐ Ensure that appropriate warning labels are printed on each and every page of the sensitive documentation.
- ☐ Prevent dumpster diving--do not discard system sensitive materials or communications in public trash containers.
- ☐ Deleting a file does not remove its data from the media. Use utilities which delete with overwriting before releasing media for other assignments or to ensure its destruction.
- ☐ Access only information for which you are authorized, “need to know/access.”
- ☐ Respect the copyright on the material you reproduce.
- ☐ Backup data files at frequent intervals.
- ☐ Respect and protect the privacy and confidentiality of records and privacy act information while in your custody.

Dial in Access:

- ☐ Dial in users must ensure that adequate safeguards are in place on the remote computer to ensure the security of the system to which you are dialing in to.
- ☐ Lock your terminal or log off if you must leave the work area even briefly.

Laptops:

- ☐ Login IDs, passwords and /or sensitive information should not be saved on the hard drive. Use a diskette/CD to save information.
- ☐ Protect passwords and user ID’s from hacker, electronic eavesdroppers or shoulder surfers.

Internet Usage:

- ☐ Do not transmit sensitive information via the internet.
- ☐ Keep your anti-virus software current.
- ☐ Periodically virus scan your client.
- ☐ Virus scan all e-mail attachments.
- ☐ Do not open executable attachments.

General:

- ☐ Use FCC computing resources when accessing applications in a manner consistent with its intended purpose.
- ☐ Report sensitive circumstances to the help desk.
- ☐ Politely challenge unescorted visitors in your area (request identification and purpose).
- ☐ Be alert to the risk of theft, espionage and intrusion in the areas you work in and take appropriate countermeasures.
- ☐ Attend or participate in annual information security training.
- ☐ Report violations of security policies or procedures that come to your attention.
- ☐ Prevent social engineering–do not reset passwords for any person via telephone until the identity of the requestor has been confirmed and verified.
- ☐ Do not divulge account access procedure to any unauthorized user.
- ☐ Users are not permitted to override technical and management controls.